ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON VISUAL CRYPTOGRAPHY SHARES

Dr.N.Radha , A.Nandhinipreetha
Department Of Computer Science, PSGR Krishnammal College For Women, Coimbatore, India

Abstract

Visual cryptography is used to keep the information secure from unauthorised person by encrypting it. The performance of the visual cryptography is measured in different ways such as pixel expansion, security, contrast, number of secret images, and the type of share generated. The main intent of this paper is to study and examine the visual cryptographic shares (i.e.) meaningless or meaningful share for binary and color images.

KEYWORDS: *Visual cryptography, secret sharing, share generation.*

INTRODUCTION

Visual cryptography is a type of encryption technique, which is used to hide the information in image in such a way that the decryption can be done by the human visual system by stacking the correct keys. This technique was first proposed by Moni Naor and Adi Shamir [1] in 1994.Visual cryptography which uses two transparent images that is called shares. The shares are generated from the image based on the pixel. Each pixel on the image is divided into smaller blocks. The probabilities of black and white pixel are same i.e. if the pixel is divided into two parts there are one black and one white block, like this the shares are generated. One share image contain random pixel and other share contain secret information. It is not possible to reveal the secret information from one image, both the shares are needed to get the secret.

Visual cryptographic technique is used for secure communication, various secrets and multimedia information are transmitted over the internet and suitable techniques are required to prevent form the illegal usage of information. This paper provides the overview of various visual cryptographic schemes based on their performance. In order to improve the security issue over the communication channel meaningful shares are used. Other performance measure such as pixel expansion, contrast, accuracy is discussed in this paper. The basic encryption and decryption process of visual cryptography is shown in the Fig. 1.

This paper is organized as follows: section II discusses about Background study for various visual cryptographic schemes and section III describes conclusion.

Encryption and decryption of visual cryptography

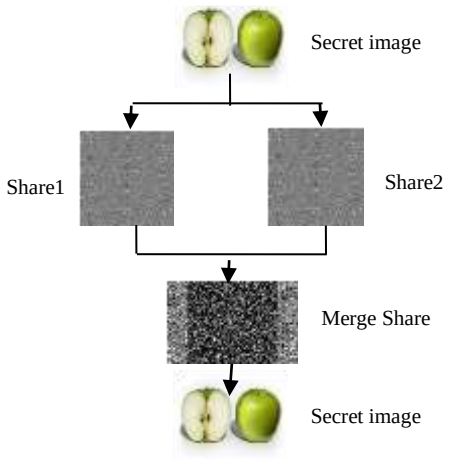

Fig. 1

BACKGROUND STUDY

1. **Visual cryptographic scheme for meaningless shares**

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Binary secret image with meaningless share

- Naor and Shamir et. al [1] was first introduced visual cryptography scheme in the year of 1994. This scheme is mainly used for securing the images. This encryption is done by 2 out of 2 visual cryptography schemes for binary images. The encryption process which involves breaking up the image into n shares. The secrets cannot be retrieved from these shares. The decryption process is completed only by combining all the shares not by the less number of shares.

- Thomas Hofmeister et. al [2] use (k, n) scheme to compute exactly the best contrast of image. The optimal trade between the contrast and the number of sub pixels will be proved by using different approach via coding theory. The main goal of this paper is to achieve security and contrast. The usage of contrast optimal scheme helps to solve the linear program problems. The efficient number of sub pixel can be achieved by constructing contrast optimal (k, n) scheme. By limiting the pixel value (i.e.) threshold value helps to reduce the pixel expansion. As a result of using these combinations of technique which helps to provide better security and it reduce the pixel expansion.
- Pei Fang Tsai et. al [3] proposed a new approach called (3,3) visual secret sharing scheme and novel cryptographic encryption scheme is also used the code book is used for the encryption. The encryption process begins by passing the three secret message in first coding share A and share temporary will be obtained from this process, then share B & C are obtained by passing share temporary in second coding. In decryption secret is obtained by combing share temporary will give secret 2.By routing share A in anticlockwise direction and combining share and temporary will give secret 3.By using this method the level of security to the image is more higher than the traditional visual cryptography.

- Zhi Zhuo et. al [4] To achieve visual cryptography via halftone provide novel encryption technique for visual cryptography scheme in binary images. In this scheme blue noise halftoning is used to generate pleasant halftoning image. The visual quality is better than compares to other scheme. This scheme can be used in number of visual secret sharing applications which needs high visual quality images.

- Sandeep katta et. al [5] uses recursive hiding scheme for 3 out of 5 secret sharing. The secret information's are selected according to their size that is smaller image to larger and vice versa. At each consecutive level the shares are distributed, it's not easy for anyone to access all the shares in the smaller image. In real cyber world the method like recursive information hiding in visual cryptography can be applied in many applications. By implanting the final decryption process in human visual system instead of complex computation is the major advantages. The 3 out of 5 recursive hiding scheme can be extended to a k out of n scheme.

- Lekhika chestei et. al [6] used 2 out of 2 visual cryptography scheme for black and white images. In this paper no other special techniques are used to maintain the contrast instead of it the aspect ratio of image has been maintained. In this scheme the single share is not enough for getting the required information. The loss of contrast is lesser than the original image. This method provides better security to the secret message.

Color secret image with meaningless share

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

- Bert W.Leung et. al [7] the scheme used in this paper splits secret images into 4 shares. The first share named black mask and the other three shares. In this paper the implementation of this method is used in the color images. The security in this scheme is mainly based on the color composition of the original secret image. This scheme provides two level security only two colors chosen from the specific color for the original secret image. This proposed method also contains the technique the proposed system have ability to recover the original secret images with high probability.

- Ching-Nung Yang et. al [8] uses the scheme named (2,n) RIVCS(region incrementing visual cryptographic scheme) to obtain the correct color for all the regions and it also used to enhance the contrast and reduce the size of shadow image with Wang's scheme. The complete secret image of this scheme is composed of multiple images because of dividing the secret image with multiple regions and every region in this scheme has an image. For enhance the contrast and to reduce the shadow size the proposed scheme is based on the conventional visual cryptography scheme. From the experimental result the proposed scheme reveals the correct for all regions and the modified (2, n) rives contains less shadow size and it also enhance the contrast.

- Denslin Brabin et. al [9] explains a visual secret sharing scheme for color images without any pixel expansion. In this scheme using encryption, the image that containing secret information is converted into multiple secret shares and by using decryption models the original image is obtained from the shares. To increase security both the model use secret keys. The ability to generate any number of shares and to maintain the visual quality of the image makes this scheme more special. The encryption method uses the generalized format for obtaining original secret image from the shares. This scheme does not use the pattern book for generating a share. This proposed scheme is evaluated using MATLAB Tool. Further increasing the security column permutation operation and secret key are generated. Human visual system is used to visualize the recovery image. No other special devices are needed.

2. Visual cryptographic scheme for meaningful shares

Binary secret image with meaningful share

- Srinivasulu et. al [10] introduced blue noise dithering principles for halftone technique. In this proposed scheme the error diffusion algorithm is used to encode a halftone share from a secret binary image which containing a significant visual information. The security property in this scheme also maintain better than the region incrementing visual cryptography and extended visual cryptography. The visual secret sharing applications which want high quality visual images are mainly applicable by this proposed method. To generate halftone shares the blue noise halftone principle is used in the conventional visual cryptography and by encryption this high quality halftone images or the shares the secret binary image is evaluated. The result of this scheme provides a better visual quality for the secret information than any other cryptography method.

- Jerripothula sandeep et. al [11] construct extended visual cryptography scheme in this paper that helps to embedding the random shares into covering images. By considering the secret image and original share image as output, the extended visual cryptography generate shares and these shares must satisfied by the bellowed criteria, from any subset of shares secret image can be

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

recovered, For obtaining secret image forbidden share cannot be used, All the shares are meaningful image. The advantages of these schemes are able to work with gray scale images, smaller pixel expansion, more secure, there are no complimentary shares. By using the general access structure, it provides more security than others. The high visual quality of shares will be achieved by using proposed scheme.

- Manesh Kumar et. al [12] used k out of n visual cryptography scheme in binary image for getting the image with less pixel expansion and pleasant image. In this scheme for getting the secret image all the n shares must be needed. The secret image cannot be obtained if suppose when the number of share is lesser than n. This paper solves the problem of pixel expansion and it generates good looking decoded images. The size of the decoded image is same as the original mages. Efficient memory space is used in the decoding process.

Color secret image with meaningful share

- Anantha Kumar kondra et. al [13] use CRC algorithm and color visual cryptographic and error diffusion method is used. This method helps to generate the quality of share and diffuses the error. Apart from these function these method also enable to provide security from threads like modification, fabrication, Interception. As a result it provides good result compared to the previous scheme. Because of using these 2 fundamental algorithms such as error diffusion and visual information pixel synchronization makes the method simple and efficient manner to generate image halftone. The visual contrast of shares and the color of image are improved by the synchronization of the visual information pixel helps to increase the security analysis of confidential information.

- Jacques Machizaud et. al [14] uses the new method of visual cryptography which based on color matching. The share image generate by this proposed method is used to detect for grey as the color of the image which kept as a secret. The spectral model is used for color reproduction that describing printed colours in an optical point of view. In addition to the secret image that revealed from the stack of the shadow image. The proposed scheme has color matching visual cryptography scheme and this scheme also contains message authentication color for the provider. This scheme helps us to provide easy expansion of n out of n visual cryptography scheme by taking into account of the optical properties in superposed supports.

- Anuprita Mande et. al [15] introduce a method called error diffusion halftone, which makes visual cryptography method easier and faster to produced meaningful color shares. Because of this error diffusion technique which give the image more pleasant to human eyes. Stucki algorithm makes the encryption and decryption method as easier as possible. The performance of this algorithm helps to reduce the time taken by the encryption and decryption method.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

TABLE1: SUMMARY OF BACKGROUND STUDY

Author	year	No of secret image	Format	Type of share	Pixel expansion	Technique	Result
Naor and Shamir	1995	1	Binary image	Meaningless	4	Visual cryptographic scheme	**Fair**
Thomas hofmeister	2000	1	Binary image	Meaningless	4	Contrast optimal k,n scheme	**Fair**
Pie-Fang Tsai	2003	3	Binary image	Meaningless	2	3,3 visual secret sharing scheme	**Fair**
Bert W.Leung	2003	1	Color image	Meaningless	2	Patten recognition	**Fair**
Zhi Zhuo	2010	N	Binary image	Meaningless	4	Novel encryption technique	**Fair**
Sandeep Katta	2010	3	Binary image	Meaningless	2^{k-1}	Recursive hiding	**Fair**
Ching-Nung-Yang	2011	N	Color image	Meaningless	7	2,n regional incrementing technique	**Poor**
Srinivasulu	2012	1	Binary image	Meaningful	4	Halftone technique	**Fair**
Anantha kumar	2012	1	Color image	Meaningful	1	Error diffusion method	**Good**
Jerripothila sandeep	2012	1	Binary image	Meaningful	Pixel expansion small	General access structure	**Good**
JacquesMachi zaud	2012	1	Color image	Meaningful	2	Classical clustered halftoning	**Fair**
Deslin Brabin	2013	1	Color image	Meaningless	1	k, n secret sharing scheme	**Good**
Maneesh kumar	2013	1	Binary image	Meaningful	1	k, n secret sharing scheme	**Good**
Anuprita Mande	2013	1	Color image	Meaningful	1	Error diffusion method	**Good**
Lekhika chettri	2014	1	Binary image	Meaningless	2	k,k visual cryptographic scheme	**Good**

CONCLUSION

In this paper various visual cryptographic techniques are studied and their performance is evaluated on four criteria, type of share, pixel, techniques and image format. Table1 is useful to make a decision on

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

an efficient cryptographic technique for particular application. The techniques like error diffusion, general access structure, k out of n visual cryptographic scheme, classical clustered halftoning technique that gives the better solution for obtaining minimal pixel expansion and efficient security. The future focus will be on usage of Biometric in visual cryptography to enhance the security.

References

1.]Naor, Shamir," Visual cryptography", EUROCRYPT, Vol. 950, pp. 1-12, 1994.
2. Thomas Hofmeister, Matthias Krause, "Contrast-Optimal k out of n secret sharing scheme in visual cryptography", Elsevier Science, Vol. 3, No. 2, pp. 471-485, 2000.
3. Pei-Fang Tsai, Ming-Shi Wang, "An (3,3) visual secret sharing scheme for hiding three secret data", Joint Conference on Information Science, Vol. 8, No. 4, pp. 632-636, 2003.
4. Zhi zhou, Gonzalo R. Arce, "Halftone visual cryptography", IEEE Transaction on Image Processing, Vol. 15, No. 8, pp. 69-77, 2006.
5. Sandeep Katta, "Recrsive Information Hiding in visual cryptography", International Journal of Computer Science and Communication, Vol. 3, No. 5, pp. 297-299, 2010.
6. Lekhika chettri," Visual cryptography scheme based on pixel expansion for black and white image", International Journal of Computer Science and Information Technology, Vol. 5, No. 3, pp. 4190-4193, 2014.
7. B.W. Leung, F. Y. Ng, "On the security of a visual cryptography for color images", Pattern Recogn, Vol. 42, No. 5, pp. 929-940, 2009.
8. Ching-Nung Yang, Hsiang Wen.Shih, "New region Incrementing visual cryptography scheme", International Conference on Image Processing, Vol. 3, No. 1, pp. 323-329, 2011.
9. Denslin Barbin,Divya Venkatesan, "Region based visual cryptography scheme for color images", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, No. 3, pp. 1473-1477, 2013.
10. Srinivasalu, K.Ramanajaneyulu, "Visual cryptography scheme using Halftone technique", International Journal of Electronics and Communication Technology, Vol. 3, No. 4, pp. 90-93, 2012.
11. Jerripothula Sandeep, Abdul Manjeed, "Embedded Extended Visual Cryptography scheme", Journal of Computer Engineering, Vol. 8, No. 1, pp. 41-47, 2012.
12. Maneesh kumar, Sourav Mukhopadhyay, "Visual cryptography for black and white image", International Journal of Information and Computation Technology, Vol. 3, No. 11, pp. 1149-1154, 2013.
13. Anantha Kumar Kondra, U.V.Rathnakumari, "An improved (8, 8)color visual cryptography scheme using Floyd error diffusion", International Journal of Engineering Research and Applications, Vol. 2, No. 4, pp. 1090-1096, 2013.
14. Jacques MachiZaud, Thierry Fournel, "Two out of Two color matching based visual cryptography scheme", The International Online Journal of Optics, Vol. 20, No. 20, pp. 22847-22859, 2012.
15. Anuprita mande, Manish Tibdewal, "A fast encryption algorithm for color extended visual cryptography", International Journal of Emerging Technology and Advanced Engineering, vol. 3, No. 4, pp. 2250-2459, 2013.
16. Sukumar Reddy, "Visual cryptographic scheme for secret image retrial", International Journal of Computer Science and Network Security, Vol. 14, No. 6, pp. 41-46, 2014.
17. Jagdeep Verma,"a visual cryptographic technique to secure image shares", International Journal of Engineering Research and Application, vol. 2, No. 1, pp. 1121-1125, 2012.
18. Shyamalendu kandar, "k-n secret sharing visual cryptography scheme on color image using random sequence", International

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Journal of Computer Applications, Vol. 25, No. 11, pp. 0975-8887, 2011.

19. Sozan Abdulla, "New visual cryptographic algorithm for colored image", Journal of Computing , Vol. 2, No. 4, pp. 21-25, 2010.
20. Dinesh Reddy, "Rotation visual cryptography using basic (2,2) scheme", International Journal of Computing Science and Communication Technologies, Vol. 3, No. 2, pp. 594-597, 2011.